Cyber-security: Why would I tell you?

Research briefing report by Mandy Messenger
13 February 2006, Version 0.3

Synopsis

This article describes the findings from research conducted in the UK into the social-psychological factors influencing the sharing of Cyber threat information.

Analysis of detailed interviews with a rich variety of security professionals, spread over one year, yielded insights into both the influences and the mental processes involved. Trust, ability, empowerment and professional confidence are key factors. In addition, the influence of expectations, reputation and perceptions of others were fundamental to the impact of key factors. Interestingly, the dominant 'frame of mind', or 'Social Identity' altered the ultimate decision making. These findings offer potential for the development of practical techniques for nurturing the sharing of sensitive information between organisations.

This report is a synopsis of an MSc paper prepared by Messenger Associates in conjunction with NISCC.
It forms the basis of continuing work within NISCC on the role of trust in information sharing.

NISCC
NATIONAL INFRASTRUCTURE SECURITY CO-ORDINATION CENTRE

Cyber-security: Why would I tell you?

Research briefing report by Mandy Messenger

1.0 The situation

There are known benefits from both public and private sectors sharing information about cyber-security threats and vulnerabilities. The aim is to mitigate the detrimental impact of cyber-security threats for both the victim organisation and to protect the nation's critical infrastructure. Yet initially, sharing might seem an altruistic act; however organisational benefits are measurable. Economists[i] in the US have taken a hard and rational look at the value of sharing within cyber-security and conclude clear benefits; particularly in competitive market places were products are interchangeable.

The importance of cyber-security is increasing, driven not only by the trend in organisations for more virtual ways of working but also because of the political considerations characterised by recent terrorist threats. A Gartner Group survey[ii] spanning 30 countries highlights that this is a global issue and results ranked 'security as the number-one technology priority for 2005.' The view from the financial industry reinforces the increasing importance of electronic security and statistics from Celent Research[iii], Boston estimate that IT security spending by North American banks will reach $1.8 billion in 2005, a 12.2% increase over 2004.

There is growing recognition, including at board level, of the importance of information security and technical warning and protection services are readily available, yet there remain urgent barriers to effective security practise. Addressing the latest cyber threat involves swift response from across the industry and that may only start following the sharing of experiences.

People have a variety of perspectives on this aspect of the security role. While some advocate sharing (for example stating that it is "necessary for the greater good"), others hold more cynical views (for example stating that it "is more trouble than it is worth!'"). Given that there are sound and rational reasons to share cyber-security information, this diversity of views implies that this is more than just a rational decision.

2.0 The response

Collaboration between security professionals involves a delicate balancing act always addressing the need to protect their organisation's proprietary interests. Investment in solid legal and contracting frameworks can form a valuable foundation but there is more to ensuring a mutually profitable sharing environment.

Many highlight the need to trust another sufficiently to share as fundamental to the mutual success of cyber security across industries. Recognising this NISCC commissioned an initial study into the social-psychological factors influencing the

sharing of cyber threat information. This was in partnership with the post graduate research programme at Birkbeck College, UCL, London. The ultimate goal is to provide guidance to those who facilitate forums. Such guidance would focus on how to develop an environment were people are both motivated and able to share. This was to include and also to go beyond the role of trust in order to consider the factors influencing the actual decision to share.

Detailed one-to-one interviews were conducted with volunteers, each person carefully selected so that the results covered as many different views and perspectives as possible. Existing forum members and facilitators were interviewed from public and private sectors, as well as the UK and US. In addition, academic, industry consultant, potential future forum members and executive managers of security leads were included in the breadth of inputs.

The volunteers explored their thinking around the decision to share (or disclose) sensitive information about a security incident or vulnerability. Interviews were spread over the last year. Each was transcribed and then coded and analysed to identify concepts and factors. As findings emerged they were compared and contrasted with published research from the field of workplace/business psychology in order to ensure insights where grounded with best practise thinking and to shape the questioning for the subsequent interviews.

3.0 The results

Back in the early 1970s psychologists[iv] suggested that the action of 'disclosure', aka sharing sensitive information, was determined by an individual's personality. The influences are more complex and situational factors play an important role and that is good news for sharing within security forums. However, the challenge is to develop that environment and the associated social expectations in order to facilitate valuable and timely sharing between members.

At the turn of the century business psychologists[v] took a more sophisticated look at disclosure. This included focusing on disclosure as an interpersonal behaviour (something that happens, over time, between two or more people) and recognised that the behaviour is normally discretionary. Why do people engage in discretionary actions? There are many factors, for example, some think that women where more likely to share than men; there is some evidence for this generally[vi] but this was not found to be evident in workplace situations[vii].

During the joint NISCC and UCL study several key areas emerged. Not surprisingly, how people were motivated and what motivated them were fundamental but so too were the decision-making and actual sharing strategies. The interviews revealed that security professionals had very sophisticated thinking around the decision to disclose and subsequent analysis developed categories of factors involved in that thinking. Ideally, to enable an open and

sharing forum, these conditions should be nurtured by those leading and facilitating the community.

Beyond these categories, the study identified key insights:

- Firstly, that it was the expectation of success or negative consequences that influenced, rather than the actual reality. These expectations were dynamic and were built through personal experience and also the reputations of others.
- Secondly, people were able to consider, at the same time, assessments of the likelihood of both positive and negative outcomes yet negative outcomes 'loomed large' in their perspectives.
- Thirdly, assessment of trustworthiness in another was crucial, but could be developed in a number of ways.
- Fourthly, personal ability and empowerment, along with having clear strategies for communicating and controlling the extent of any disclosure, are necessary to mitigate the risk of negative outcomes.
- Finally, the current 'frame of mind' of an individual tended to alter how they combined these factors when reaching their decision to disclose or withhold information.

Details of the development of trust, the abilities and the conditions for the different 'frames of mind' developed during the study. This report details these findings in turn and proposes implications for the facilitation of such sharing forums:

3.1 Developing Trust:

Those interviewed had a high awareness of need for trust between parties. A number of different types of trust were reported. The first is **Deterrence-Based** trust[viii] which is that you can trust someone to do as they say they will as they 'fear' a punishment. Legal frameworks can provide this sort of trust but for this situation it was not enough. Still needed but not sufficient; other sorts of trust were also required.

Next is **Calculus-Based**[ix] where the motivation is to obtain rewards. In some cases the rewards of reciprocal sharing might be at some indeterminate point in the future - so again this is not enough.

Knowledge-Based trust, (which is about 'knowing' another person well enough to predict their behaviour) was reported as the most suitable type of trust. It is likely to develop over time, through interacting with the person. It is the personal relationship that has the weight, not an organisational role, so consistency of membership is necessary. Interestingly, whereas this trust normally requires meeting and spending time with people, in the interviews it seemed more important to have seen how they handle themselves in difficult situations, not only in holding on to secrets but also behaving ethically to others who have

secrets and who might be more naive. This sort of trust requires an investment of time, however once established it is more tolerant of slight changes in behaviour, because this behaviour is put down to the situation a person was in rather than being a flaw in the person themselves[x].

During the interviews expectations about the integrity of other security professionals were high and this can provide a limited degree of **Identification-Based** trust. This is when you "identify with the other's desire and intentions" to the extent that they can act as your proxy. One useful type of trust development mentioned was when a well-respected peer was able to introduce and recommend another person. This would then provide an initial level of trust. This was a form of **Pre-emptive or Referential Based**[xi] trust which could be used selectively in the development of a sharing forum.

3.2 Abilities & strategies

Trust is an attribute of a relationship and, for sharing information, trust needs to be expressed through action. Even once trust is in place, the expression of trust is mediated by role **autonomy** (the discretion that people have in interpreting and enacting their roles)[xii]. The behaviour of any person is constrained by the position they hold within an organisation[xiii]. Autonomy of security professionals was reported to be critical.

Clearly the holder of information needs to be empowered to share. However, empowerment is also important for the recipient of information. For shared information to be fruitful requires empowerment in two domains - empowerment from the forum, to make use of what has been shared, but also to be empowered back in the work place, or home organisation, to make changes or investments in response to that information.

It was recognised that information has value to the recipient as well as a risk to the sharer so ways to maintain the value while reducing the risk are necessary but can provide a paradox. **Anonymising** information might defend the sharing organisation but it also reduces the weight or authority of the information to any recipients. As defending against a potential violation might require the investment of significant resources, the credibility of sources is important. Partial anonymisation, and/or the brokering of information via mutually trusted 3rd parties were considered useful techniques.

Interviewees viewed information as a commodity, which has a value as part of an exchange. While they where motivated to share as part of identification with the forum goals and defending the nation's critical infrastructure, they also report their expectation that they, in return, will receive some information of value. They did recognise that the timing of any return might be considerable. Interviewees were highly aware that there might always be a certain amount of information that they would never be prepared to share.

However this was only true at a macro level. When looking at what was shared, moment to moment (at the micro level) on the details of a particular incident, a highly controlled process was expected where each party gradually revealed information. An analogy was used with a game of poker in that there is an aim to minimise exposure yet to maximise gain.

3.3 The influencing 'Frames of Mind'

Part of the analysis of the interview transcripts allowed a theory to be proposed as to how the interviewees combined these different factors to make their overall decision. Different people had different beliefs about sharing even though they were aware of the same factors. While each person has beliefs and expectations about how hard and how successful and how risky sharing might be the decision process seems to be more than just adding the various factors together.

Some bias or weighting of the factors appeared to be part of the process. Each of us has many roles, each with particular responsibilities. Psychologists call these our Social Identities[xiv]. The Social identity that was the forefront of their mind seemed to be influencing the decision process. If a person is currently thinking about their job they appear to find the risks and the potential barriers clear in the focus of their mind, while the benefits would recede into the background[xv] . If they are thinking in the context of the need for a professional sharing forum in support of a well-defended critical infrastructure then they are more likely to consider benefits and the value of the work.

This theory does not imply that the 'frame of mind' would leave the individual blind to any factors, but merely that they would experience some factors as 'looming large' in their thinking. The result is a shift in the balance of the motivation to share, and the expectation of their ability to do so, leading to a successful outcome without personal or organisational harm.

4.0 The next steps

The next step is to apply this understanding to active sharing forums and to test out the proposed theories. NISCC is considering the implications of the outputs of this study. If you would like to be involved please do email the NISCC contact on Sharing@niscc.gov.uk. In addition, NISCC along with ETR^{2}A (www.**etr2a**.org) and Messenger Associates are exploring projects to develop the understanding of the role of trust between government and industry as an enabler for the sharing of cyber threat information. Mandy Messenger conducted this research study and is keen to support the development of sharing cultures within the cyber security industry. If you would like to know more she can be contacted on mandy@messengerassociates.co.uk.

[i] **Gal-Or, E. & Ghose, A. (2005)** The Economic Incentives for Sharing Security Informatio, Information Systems Research, Vol. 16 (2), Page s186-209.

[ii] **Newman, K. (2005)** Risky Business, New Zealand Management, Vol. 52, Issue 6, Pages 68-70

[iii] **Bielski, L. (2005)** Security breaches hitting home, ABA Banking Journal, Vol. 97, Issue 6, Pages 7-10.

[iv] **Jourard, S. M. (1971)** The transparent self. New York: Van Nostrand.

[v] **Omarzu, J. (2000)** A Disclosure Decision Model: Determining How and When Individuals will self-disclose, Personality and Social Psychological Review, Vol 4, No 2, Pages 174-185.

[vi] **Dindia, K. & Allen, M. (1992)** Sex differences in self-disclosure: A meta-analysis, Psychological Bulliten, Vol 112, Pages 106-124.

[vii] **Young, J.W. (1978)** The Subordinate's Exposure of Organizational Vulnerability to the Superior: Sex and Organizational Effects, The Academy of Management Journal, Vol. 2 (1), Pages 113-122.

[viii] **Shapiro, D., Sheppard, B. H. & Cheraskin, L. (1992)** Business on a Handshake, Negotiation Journal, Vol 8(4), Pages 365-377.

[ix] **Lewicki, R.J. & Bunker, B.B. (1996)** Developing and Maintaining Trust in Work Relationships in Kramer R. M. & Tyler T. R. (eds.) Trust in Organisations :Frontiers of Theory and Research'. Thousand Oaks, CA: Sage.

[x] **Lewicki, R.J. & Bunker, B.B. (1996)** Developing and Maintaining Trust in Work Relationships in Kramer R. M. & Tyler T. R. (eds.) Trust in Organisations :Frontiers of Theory and Research'. Thousand Oaks, CA: Sage.

[xi] **Kramer, R.M. (1999)** 'Trust and Distrust in Organisations: Emerging Perspectives and Enduring Questions', Annual Review Psychology, Vol. 50, Pages 569-98.

[xii] **Perrone, V., Zeheer, A. & McEvily, B. (2003)** 'Free to be trusted? Organizational constraints on trust in boundary spanners', Organisational Science, Vol 14(4) Pages 422-439.

[xiii] **Simon, H (1945)** Administrative Behaviour: A study of decision-making processes in administrative organization. New York: Free Press.

[xiv] **Tajfel, H. (1972)** Social Categorisation. English manuscript of 'La categorisation sociale', In Moscovici, S. (Ed.) Introduction á la Psychologie Sociale, Vol 1, Pages 272-302.

[xv] **Nevis, E.C. (1998)** Organisational Consulting: A Gestalt Approach, Cambridge, MA: GICPress.